



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Romania

COUNTRY **Romania**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **21 October 2026**

KEY REGULATORS **National Authority for Management and Regulation in Communications · National Cyber Security Directorate · National Supervisory Authority for Personal Data Processing**

Key takeaways

- Romania has no general telecom licence. A company that offers public mobile, fixed or internet services notifies the telecom regulator, ANCOM, no later than the day it starts, using a signed electronic form.
 - Romanian law does not require operators to identify prepaid SIM buyers. Parliament and the Government tried to make it mandatory twice, and the Constitutional Court struck down both attempts (2014 and 2020).
 - Telecom operators are not covered by Romania's anti-money laundering law. Any identity check at SIM sale or SIM swap is the operator's own security and fraud control, not a legal know-your-customer duty.
 - Online sales are allowed. A postpaid contract can be signed at a distance with a qualified or advanced electronic signature, and a number can be ported remotely if the new operator can verify the account holder remotely.
 - Since 31 December 2024, network security falls under Romania's NIS 2 cybersecurity law. Operators must register with the National Cyber Security Directorate, warn it of significant incidents within 24 hours, and face fines of up to 10 million euro or 2% of worldwide turnover.
-

The Romanian market is open to new mobile, MVNO and eSIM providers, including providers established elsewhere in the EU. Entry works by notification rather than licence (spectrum and numbering resources are assigned separately), and online sales channels are expressly recognised in the electronic communications law.

Three authorities matter most. The National Authority for Management and Regulation in Communications (ANCOM) regulates services, numbering and portability. The National Cyber Security Directorate (DNSC) enforces the NIS 2 framework, with ANCOM as sectoral authority for telecom. The data protection authority (ANSPDCP) supervises personal data, including the telecom-specific privacy law.

The main obstacle for a new entrant is not identity regulation, which is light. It is the volume of sector rules: number portability within one working day with compensation for failures, NIS 2 registration and incident reporting, and ANCOM's security and anti-fraud measures, which an online-only provider must build into its systems from day one.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Authority	Remit	Level	Official site
National Authority for Management and Regulation in Communications (ANCOM)	General authorisation, numbering, number portability, end-user protection, sectoral cybersecurity authority for telecom under NIS 2, Digital Services Coordinator	National (autonomous authority under parliamentary control)	ancom.ro
National Cyber Security Directorate (DNSC)	NIS 2 competent authority: registration, incident reporting, supervision and fines	National	dnsc.ro
National Supervisory Authority for Personal Data Processing (ANSPDCP)	GDPR and Law 506/2004 on privacy in electronic communications; personal data breaches	National	dataprotection.ro
National Authority for Consumer Protection (ANPC)	General consumer law, which applies to telecom consumer contracts alongside the sector rules	National	anpc.ro
European Union	European Electronic Communications Code, NIS 2 Directive and GDPR	Supranational	eur-lex.europa.eu

ANCOM was set up by Government Emergency Ordinance (OUG) no. 22/2009 as an autonomous public authority under parliamentary control, funded entirely from its own revenue (art. 1). The framework law is OUG no. 111/2011 on electronic communications, approved with amendments by Law no. 140/2012 and amended most significantly by Law no. 198/2022, which transposed the European Electronic Communications Code. Romania is a unitary state, so every authorisation is national.

2 Licensing and authorisation

Public electronic communications networks and publicly available services are provided under a **general authorisation**, set by ANCOM President's Decision no. 70/2023 (Official Gazette Part I no. 131 of 15 February 2023) **In force**. There is no licence application or approval decision. The provider files a standard notification form, signed with an advanced electronic signature based on a qualified certificate, by e-mail to ANCOM **no later than the day the activity starts**. The procedure is free of charge, and changes to the notified data must be reported within 10 days. Providers headquartered in another EU or EEA state but not established in Romania attach their home-state identification documents. ANCOM's public register listed 572 providers of public networks and services on 31 December 2025.

Number-independent interpersonal communications services (app-based messaging and calling that does not use numbers from the National Numbering Plan) are outside the notification obligation. Two separate rights are needed for resources: **licences for numbering resources** (an MVNO or eSIM provider issuing its own numbers needs these) and **licences for radio frequencies**, which may be awarded through competitive selection procedures under OUG 111/2011.

Providing services without notification, or breaching the general authorisation conditions, is a contravention under art. 142 of OUG 111/2011 and is fined under art. 143 (see section 9). Since OUG no. 155/2024, providers of public networks and services must also register with DNSC under the NIS 2 framework (section 7).

3 Identity framework (AML rules do not apply)

Telecom operators are **not reporting entities** under Law no. 129/2019 on preventing and combating money laundering and terrorist financing. Art. 5(1) lists credit and financial institutions, private pension fund administrators, gambling providers, professionals such as auditors, notaries and lawyers, company service providers, real estate agents, and traders in goods or services where cash transactions reach the lei equivalent of 10,000

euro. Electronic communications providers are not among them. An operator falls under the law only by doing something else that is listed, for example acting as a payment institution, an e-money issuer or an agent or distributor of one (art. 5(2)).

Instead, identity in Romanian telecom is shaped by three things:

- **Contract law in OUG 111/2011.** Consumer services are supplied under a written contract (art. 50(1) and (3)): on paper, as an electronic document signed with a qualified or advanced electronic signature, or by means of distance communication. Prepaid services are the exception: the provider only hands over the general conditions on paper or another durable medium at the time of purchase (art. 50⁷).
- **No prepaid registration.** The 2014 law that would have required registration of prepaid card users and storage of their data was declared unconstitutional in its entirety by Constitutional Court Decision no. 461 of 16 September 2014 (Official Gazette no. 775 of 24 October 2014). OUG no. 62/2019, which tied the collection of prepaid users' identification data to reducing abusive 112 emergency calls, was declared unconstitutional in its entirety by Decision no. 83 of 18 February 2020 (Official Gazette no. 204 of 13 March 2020). No later act has reintroduced the obligation (as of October 2026).
- **Portability and anti-fraud rules.** Identity data must match before a number can leave the old operator, and ANCOM's security rules require logging of access and fraud (sections 4 and 7).

There is therefore no legal customer due diligence, beneficial ownership check, transaction monitoring or suspicious transaction reporting duty for telecom services as such. Operators still comply with EU and national sanctions, which apply to everyone.

4 Identity verification and onboarding

Because Romanian law prescribes no subscriber identification method, operators decide what to check and how, within data protection limits. The legal touchpoints where identity matters are these:

Signing a postpaid contract

Paper, electronic signature (qualified, or by exception advanced) or distance means "under the conditions laid down by law" (art. 50(3) OUG 111/2011, letter b as amended by Law 214/2024). The signature, not a separate ID check, is what the law requires for validity.

Buying prepaid

No identification and no contract. General conditions, standard tariff and contact details are provided on a durable medium at purchase (art. 50⁷).

Porting a number

The donor operator may refuse a port if the subscriber's identification data are incorrect or do not match the number, or, for mobile numbers, if the SIM is reported lost or stolen; for prepaid numbers, if no call was ever made or received (art. 8(2), ANCOM Decision 144/EN/2006).

Validating the port

ANCOM states that the acceptor checks the applicant's documents (identity documents, invoices, affidavits) and, for prepaid numbers, the SIM card series.

The figure below shows a typical online flow; only the signature, porting checks and prepaid conditions are legal requirements.

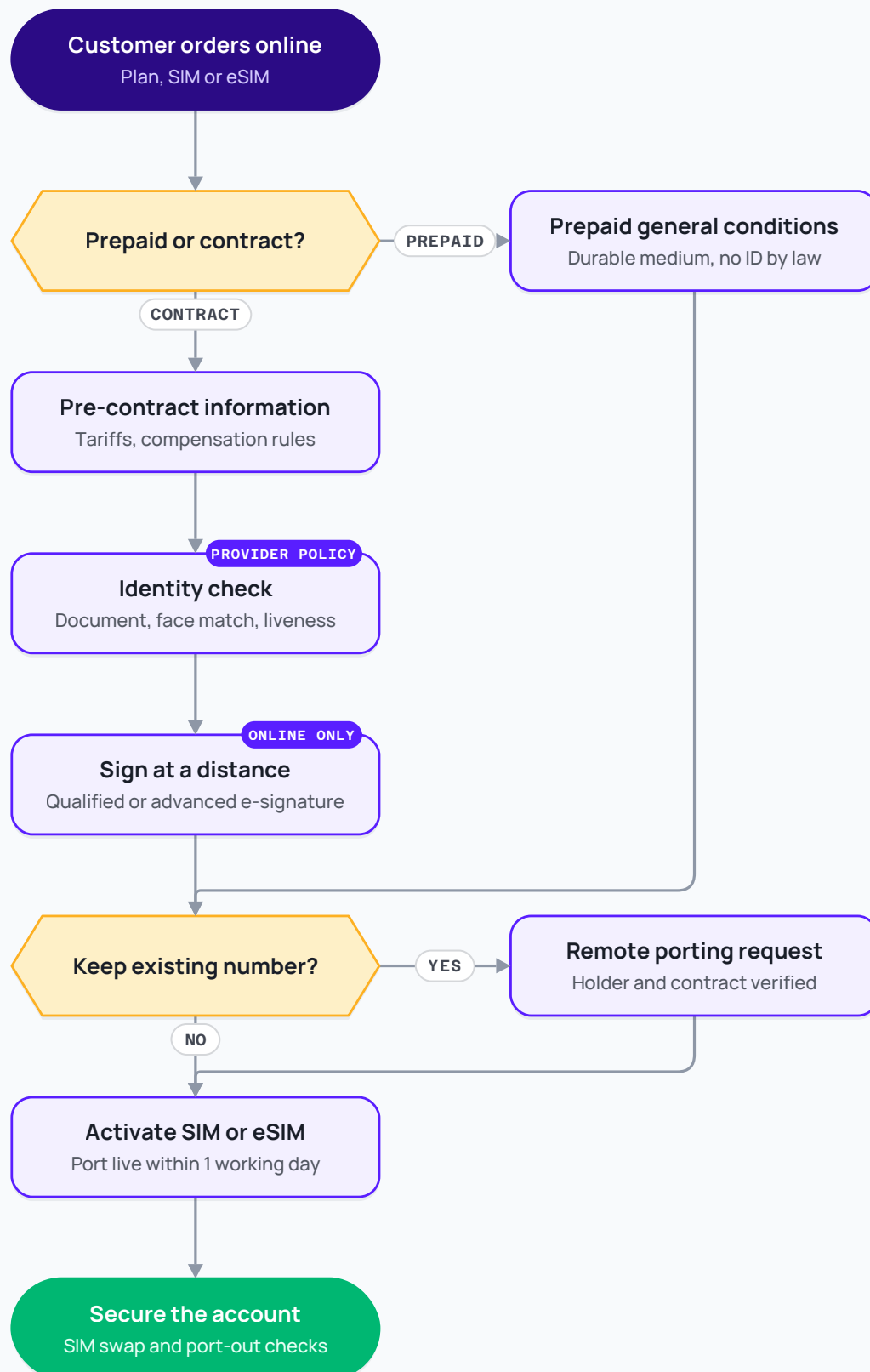


Figure 1. Online SIM or eSIM onboarding in Romania, with optional number porting.

Bottom line: Romanian telecom rules are largely channel-neutral, but they set specific conditions for the two steps that move online: signing a contract at a distance needs a qualified or advanced electronic signature, and a remote porting request is valid only if the new operator can verify the holder remotely.

Requirement	In store	Online / remote	Difference
Authorisation to provide the service	General authorisation by notification	Same notification; no separate online licence	Same
Prepaid SIM identification	Not required by law	Not required by law	Same
Postpaid contract form	Written contract on paper	Electronic document with qualified or advanced e-signature, or distance means	Differs
Porting request	Standard form at the new operator	Allowed only if holder and contract can be verified remotely	Differs
Porting cancellation and compensation claims	At the operator	Must be accepted remotely if remote port requests are accepted	Differs
Porting deadline and compensation	Activation within 1 working day of agreed date	Same	Same
Network and information security	OUG 155/2024 (NIS 2)	Same	Same

Signing at a distance

Art. 50(3) of OUG 111/2011 lists three valid forms for a consumer contract: paper; with the end-user's agreement, an electronic document signed with a qualified electronic signature or, by exception, an advanced electronic signature; or distance communication under the conditions set by law. Letter (b) was amended by Law no. 214/2024 on electronic

signatures, with effect from 8 October 2024. For app-based onboarding this means the signature flow, not the identity check, is where legal validity is decided.

Remote porting

Under ANCOM's portability rules as amended by Decision no. 72/2023, a new operator may accept porting requests by remote means only if it can verify remotely that the requester is the contract holder or legal representative and that the number is under contract with the current operator. Operators that accept remote requests must also accept cancellations and compensation claims remotely (Decision 72/2023, art. 6(1)). Porting normally takes place on the third working day; the subscriber may choose a later date, but no more than 25 working days after the request.

Prepaid and eSIM

The absence of a registration duty applies equally to physical SIMs and eSIM profiles sold online. The only statutory obligation at sale is to provide the general conditions on a durable medium (art. 50⁷), which an app or e-mail can satisfy.

6 Data protection and biometrics

The GDPR (Regulation (EU) 2016/679) applies directly, and Law no. 190/2018 (Official Gazette no. 651 of 26 July 2018) adds national implementing rules. Because there is no legal duty to identify subscribers, an operator cannot rely on "legal obligation" as the basis for collecting identity documents or selfies: it needs another basis, such as performance of the contract or legitimate interest in fraud prevention, and must keep collection proportionate.

Face matching for identification uses biometric data "for the purpose of uniquely identifying a natural person", a special category under art. 9(1) GDPR, which is processed only under an art. 9(2) exception, typically explicit consent. Operators therefore usually offer a non-biometric alternative.

Law no. 506/2004 on privacy in electronic communications adds sector rules supervised by ANSPDCP. Providers must take security measures, notify personal data breaches to ANSPDCP without delay and, where privacy may be affected, to subscribers, and keep a register of breaches (art. 3). Location data other than traffic data may be processed only when anonymised or with prior consent for a value-added service (art. 8).

Number portability

Art. 75 of OUG 111/2011 gives every end-user with a National Numbering Plan number the right to keep it when switching provider, for at least one month after ending a contract. Providers may not charge end-users for porting. The new provider activates the number within **one working day** of the date expressly agreed with the user, and service may not be interrupted for more than one working day; if porting fails, the old provider reactivates the number (art. 75(5)-(7)). ANCOM must ensure ports do not happen without the user's agreement and sets compensation rules (art. 75²(5)-(6)).

Under Decision 72/2023, compensation is **5 lei per day per number** (for mobile subscriptions and for each prepaid card) when activation is late by more than one working day or service is interrupted for more than one working day. When a number is ported **without the subscriber's consent**, the old provider pays (art. 5). Claims may be filed within 60 days of the porting date (art. 6(2)). The detailed procedure is in ANCOM Decision 144/EN/2006, consolidated on 7 May 2025 after Decision 149/2025 added rules for operator reorganisations.

Cybersecurity under NIS 2

OUG no. 155/2024 **In force**, approved by Law no. 124/2025, transposes Directive (EU) 2022/2555. It applies to providers of public networks and publicly available services whenever they provide services in Romania, wherever they are established (art. 7(2)). Large and medium-sized providers are **essential entities** (art. 5); smaller ones are **important entities** regardless of size (art. 6). Obligations include:

- proportionate technical, operational and organisational risk-management measures (art. 11);
- notification to DNSC for registration within 30 days of becoming subject to the ordinance (art. 18(2)), under DNSC Order no. 1/2025;
- for significant incidents, an early warning within 24 hours, an incident notification within 72 hours and a final report within one month (art. 15).

ANCOM is the sectoral competent authority for telecom and cooperates with DNSC (art. 37(1)(a)). OUG 155/2024 repealed the security chapter of OUG 111/2011 (arts. 46 to 49²) from 31 December 2024, but the measures in ANCOM Decision no. 70/2024 on network security remain in force until revised (art. 64(1)). That decision sets annexed security domains (including logical access control with logging of fraud) and incident thresholds of 5,000 users for 60 minutes or 500,000 user-hours.

Caller ID spoofing

From 7 July 2025, providers interconnected with networks abroad must block calls from outside Romania that display a National Numbering Plan number outside the 06 and 07 ranges, or a +40 number that does not follow the National Numbering Plan, unless they can establish that the number is used legitimately (for example, roaming users).

8

Risk indicators and red flags

TELECOM FRAUD AND IDENTITY-ABUSE INDICATORS

- **Port request with mismatched data:** identification data that do not match the number, a ground for refusal.
- **Port of a lost or stolen SIM:** a port request for a mobile number whose SIM has been reported lost or stolen.
- **Dormant prepaid number ported:** a prepaid number with no call made or received, a ground for refusal.
- **Several port requests for one number:** concurrent requests, which must be refused.
- **Spoofed Romanian caller ID from abroad:** international calls displaying national numbers, used in impersonation scams.
- **Calls impersonating banks or authorities:** callers asking users to send an SMS, type a code or share personal data.
- **International call-back lures:** missed calls from unknown international numbers to destinations with high tariffs.

9

Enforcement and penalties

Electronic communications law. Contraventions under art. 142 of OUG 111/2011 are fined under art. 143(1): from 5,000 lei to 60,000 lei, or up to 100,000 lei for repeated breaches; for providers with turnover above 3,000,000 lei, up to 5% of turnover, or up to 10% for repeated breaches. In 2025 ANCOM sanctioned 23 providers for failing to meet their statistical reporting obligations for 2024.

NIS 2. Under art. 60 of OUG 155/2024, essential entities face fines from 10,000 lei up to 10,000,000 euro or 2% of worldwide annual turnover, whichever is higher; important

entities from 5,000 lei up to 7,000,000 euro or 1.4% of worldwide annual turnover. The fines apply to the contraventions listed in art. 60(1); art. 60 took effect 30 days after publication (art. 64(4)).

Data protection. Breaches of the GDPR and of Law 506/2004 are sanctioned by ANSPDCP under its own regime.

10 Recent changes and what to watch

- **6 July 2026:** **In force** Law no. 123/2026 amends art. 36 of OUG 155/2024 (DNSC consultative committee). No change to operators' obligations.
- **27 November 2025:** **In force** DNSC Order no. 3/2025 sets the norms for supervision, verification and control and the risk-based prioritisation of inspections. Operators should expect risk-ranked NIS 2 audits.
- **2025:** **In force** DNSC Orders no. 1/2025 (registration notification) and 2/2025 (disruption thresholds and entity risk methodology). Registration with DNSC is a live obligation.
- **10 July 2025:** **In force** Law no. 124/2025 approves OUG 155/2024 with amendments; the consolidated text applies from this date.
- **7 July 2025:** **In force** Mandatory blocking of spoofed Romanian caller IDs on calls from abroad.
- **7 May 2025:** **In force** ANCOM Decision 149/2025 adds rules on number portability when operators merge or reorganise.
- **31 December 2024:** **In force** OUG 155/2024 transposes NIS 2 and repeals the telecom security chapter of OUG 111/2011; ANCOM Decision 70/2024 continues to apply until revised.

11 What this means for identity verification

- **No mandated method.** No Romanian act prescribes documents, liveness or assurance levels for subscribers, so identity checks at SIM sale are a risk-based design choice, justified under the GDPR rather than under a legal duty.
- **The signature is the legal gate.** Online postpaid contracts need a qualified or (by exception) advanced electronic signature; build the identity step to support it.

- **Remote porting needs remote verification.** To accept port requests online, the new operator must be able to verify the holder and the contract remotely; checks should match the donor's data, since mismatches are refusal grounds.
- **Unauthorised ports cost money.** A port without consent triggers daily compensation, which makes strong authentication before port-out and SIM replacement a direct cost control.
- **Biometrics need a basis.** Face matching is special-category processing; obtain explicit consent and offer an alternative.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote identity checks for online SIM and eSIM sales, with ID document capture and verification (including NFC), face match and biometric liveness.
- E-signatures to support distance conclusion of postpaid contracts.
- Verification of the account holder before remote porting, SIM replacement or port-out, using face match against the identity captured at onboarding.
- Phone and email verification and configurable no-code workflows, with cloud, on-premises or hybrid deployment to fit data protection requirements.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice** [Emergency Ordinance 111/2011 on electronic communications], Official Gazette Part I no. 925 of 27 December 2011, consolidated text, arts. 50, 50⁷, 75, 75², 142, 143, Legislative Portal, legislatie.just.ro
- **Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil** [Emergency Ordinance 155/2024, NIS 2 framework], Official Gazette Part I no. 1332 of 31 December 2024, approved by Law 124/2025, consolidated text, arts. 5, 6, 7, 11, 15, 18, 37, 60, 64, Legislative Portal, legislatie.just.ro
- **Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea ANCOM** [Emergency Ordinance 22/2009 establishing ANCOM], art. 1, Legislative Portal, legislatie.just.ro
- **Curtea Constituțională, Decizia nr. 461 din 16 septembrie 2014** [Constitutional Court Decision 461/2014], Official Gazette no. 775 of 24 October 2014, Legislative Portal, legislatie.just.ro
- **Curtea Constituțională, Decizia nr. 83 din 18 februarie 2020** [Constitutional Court Decision 83/2020 on OUG 62/2019], Official Gazette no. 204 of 13 March 2020, Legislative Portal, legislatie.just.ro
- **Decizia ANCOM nr. 72/2023** [ANCOM Decision 72/2023 on compensation for number portability failures], Official Gazette no. 130 of 15 February 2023, arts. 5 to 7, Legislative Portal, legislatie.just.ro
- **Decizia nr. 144/EN/2006 privind implementarea portabilității numerelor** [ANCOM Decision 144/EN/2006 on number portability], unofficial consolidation in force on 7 May 2025, art. 8, ANCOM, ancom.ro
- **Decizia ANCOM nr. 70/2024 privind securitatea rețelelor publice de comunicații electronice** [ANCOM Decision 70/2024 on network security], 1 February 2024, Official Gazette no. 117 of 9 February 2024, ancom.ro
- **ANCOM, Notification procedure** (general authorisation, Decision 70/2023, Official Gazette no. 131 of 15 February 2023), ancom.ro
- **ANCOM, Number portability**, ancom.ro
- **ANCOM, Number Portability explained step by step**, press release, 28 May 2024, ancom.ro
- **ANCOM, measures against fraud through calls made on behalf of public institutions, banks or state-owned companies**, press release, 4 June 2025, ancom.ro
- **ANCOM, From July 7, fewer phone calls with falsified identity**, press release, 4 July 2025, ancom.ro
- **ANCOM, new rules for numbering resources and number transfers between operators** (Decision 149/2025), press release, 10 April 2025, ancom.ro
- **ANCOM, Raport anual 2025** [Annual report 2025], pp. 29 and 31, ancom.ro
- **ANCOM Infocentru, Fraud and data security**, infocentru.ancom.ro
- **Legea nr. 198/2022** [Law 198/2022 transposing the European Electronic Communications Code], Official Gazette Part I no. 681 of 7 July 2022, ancom.ro
- **DNSC, Legislație NIS 2** [NIS 2 legislation, including DNSC Orders 1/2025, 2/2025 and 3/2025], dnsc.ro

- **Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului** [Law 129/2019 on AML/CFT], Official Gazette Part I no. 589 of 18 July 2019, art. 5, asfromania.ro
- **Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice** [Law 506/2004 on privacy in electronic communications], Official Gazette no. 1101 of 25 November 2004, arts. 3 and 8, dataprotection.ro
- **Legea nr. 190/2018** [Law 190/2018 implementing the GDPR], Official Gazette no. 651 of 26 July 2018, dataprotection.ro
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, art. 9, eur-lex.europa.eu
- **Directive (EU) 2022/2555 (NIS 2 Directive)**, art. 43, eur-lex.europa.eu